ASSURED
ENTERPRISES INC

Comment being submitted by Assured Enterprises, Inc., Austin, Texas, for the following Federal Register post:

Agency Information Collection Activities: Information Collection Renewal; Submission for Review; FFIEC Cybersecurity Assessment Tool

A Notice by the Comptroller of the Currency on 12/16/2015

OMB Number: 1557-0328
Document No. 2015-31583
Document Citation: 80 FR 78285

We at Assured Enterprises, Inc. have recently become aware with great interest of the FFIEC Cybersecurity Assessment Tool and wish to comment on its effectiveness for securing the nation's banking and financial services (BFS) industry.

Banking and financial services (BFS) institutions represent a major component of the nation's Critical Infrastructure. Faced with evolving, sophisticated cyber threats, the industry should bring to bear the most advanced technology available.

We note that it is difficult for US Government Agencies to remain at the cutting edge of technological developments and thus appreciate the opportunity to discuss a few thoughts regarding the FFIEC Cybersecurity Assessment Tool.

It may be worth noting that for a few years the U.S. Defense Information Systems Agency’s (DISA) Gold Disk vulnerability analysis tool served as the benchmark for assessments. Today, anyone relying on this tool alone is inviting calamity. The Gold Disk provides an automated mechanism to assess and compare a computer network operating system with the compliance specifications of the Security Technical Implementation Guide (STIG).

However, in December 2012, further development of Gold Disk ceased. As a legacy tool, Gold Disk supports Windows XP, Windows Vista, Windows 2003, Windows 2008 R1. There are no plans to develop Gold Disk for future technologies or products, including Windows 7 and beyond. In the future, Field Security Operations (FSOs) will transition to Security Content Automation Protocol (SCAP) standards for compliance reporting involving Windows 7 and other operating system rollouts. SCAP defines standards to enable automated vulnerability management, measurement, and STIG compliance. Thus, Gold Disk is a legacy product which examines operating system configurations and which provides some compliance information. The BFS industry and its regulators should learn from this experience and insure that reliance on less than state-of-the-art assessment tools should be avoided.

Currently DISA has adopted the Assured Compliance Assessment Solution (ACAS) an integrated software solution that does not address the state-of-the-art proactive, binary level assessment technique, Deep Software Scanning. The ACAS suite of enterprise tools provides automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery. However, it only scans for common vulnerabilities and exposures.

Today, the vast majority of successful cyber-attacks exploit known vulnerabilities hidden within user software applications or mission system software. Today's problem is not system configuration or mechanical compliance. Today's problem is the Known Vulnerabilities lurking within the binaries making up the software in use today.

It is important to note that the field of vulnerability assessments is comprised of several different types of tools, which may accurately be compared as apples, oranges and bananas.

For example, the class of application security testing systems may be seen as bananas - unique when compared to another class - vulnerability assessment tools. Examples of application security testing systems include White Hat, IBM AppScan, and HP WebInspect.

The more closely related apples and oranges are the Vulnerability Assessment tools. For example, there are some tools (oranges) which address only network configuration issues. While network configuration errors may give rise to gaps and vulnerabilities, the fact remains that comparatively few successful attacks today exploit these gaps and vulnerabilities. The overriding issue should be cost-efficiency and efficacy.

If we turn to the apples, we discover that today a significant majority of the successful attacks against corporate America arise from exploitation of KNOWN VULNERABILITIES LURKING WITHIN THE SOFTWARE running on networks and systems. This assessment is based on studies by Verizon, Sans Institute, Ponemon and others.

Thus, the apple of our eye in terms of Known Vulnerabilities ought to be those tools which actually address the genuine threats faced today. This general area is known as software application scanning. Until very recently, the best software scanners on the market were those which were used by software developers for the design, coding and testing phases of software development. But for technological reasons, none of those devices could look at the binaries which make up the software code. This is a very important distinction, because during the software development process open source code, various DLLs and other extensions, frequently, may be innocently slipped into the code to solve a problem. The belief by the developer is that such additions have been vetted. However, since the creation of the NIST Database of Known Vulnerabilities, the number of KNOWN software vulnerabilities alive and well at the code level have grown to over 200,000. New Known Vulnerabilities are added practically daily. Thus static systems are inadequate. Until recently there was no tool on the market to assess these Known Vulnerabilities. Thus, such assessments were either conducted manually or not at all.

But a new class of tools on the market—Deep Software Scanners—are proactive, binary-level, non-signature based application vulnerability assessment tools—are simply game changing. The FFIEC should recognize this new class of tool—Deep Software Scanners. To our understanding, this class of tools can run automatically and produce a series of reports, typically overnight. The older software scanners would take days, even weeks to complete their runs and would not address known vulnerabilities in the software binaries. This new class of Deep Software Scanner detects known vulnerabilities in the binaries comprising the software and application codes running on extant systems.

This new class of Deep Software Scanner yields reports which detail the best practice remediation steps for each vulnerability (something which is foreign to other classes), and this class of tool provides both information about the attack vectors which have been used in the past to exploit each vulnerability, but more importantly, information regarding the risk or threat level associated with each such vulnerability. Reliance on the NIST database yields only generic prioritization of each detected vulnerability. However, there are firms which have figured out how to rapidly and cost-effectively tailor the prioritization finding to reflect the actual cyber maturity on the system being tested. This system, taken as a whole, represents the new gold standard in software vulnerability assessment.

The Apples of the Teacher’s Eye are the Deep Software Scanners. The best of these Deep Software Scanners: (1) detects known vulnerabilities in all major operating systems, including Windows, Apple, Linux, Solaris, UNIX, etc., (2) provides a critical assessment of the identified vulnerabilities, (3) provides a narrative to illustrate the foreseeable exploits of each vulnerability and (4) details recommended corrective or remediation actions so that the user can decide when and how to address the most important vulnerabilities identified. Deep Software Scanners are unique because they can scan applications and mission system software on a hunt to identify and show how to eradicate over 200,000 known software vulnerabilities.

Deep Software Scanning—proactive, binary-level, non-signature based application vulnerability assessment tools—ought to be the *sine qua non* of vulnerability assessment for the FFIEC Cybersecurity Assessment Tool.

Deep Software Scanners are the new cybersecurity Gold Standard for Effective Vulnerability Assessment and Correction.

We are available to supply additional information, upon request.

Yours in a Secure America,

Stephen M. Soble, CEO
Assured Enterprises, Inc.
7300 RM 2222
Building Three, Suite 100
Austin, TX 78730
Email: info@assured.enterprises

www.assured.enterprises